



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10065662 A**

(43) Date of publication of application: 06 . 03 . 98

(51) Int. CI

H04L 9/08
G11B 20/14
H04L 9/14
H04L 9/32
H04N 7/24

(21) Application number: **09082598**

(22) Date of filing: 01 . 04 . 97

(30) Priority: 01 . 04 . 96 JP 08 78647
10 . 06 . 96 JP 08147272

(71) Applicant: **SONY CORP**

(72) Inventor: **ISHIGURO RYUJI**
OSAWA YOSHITOMO

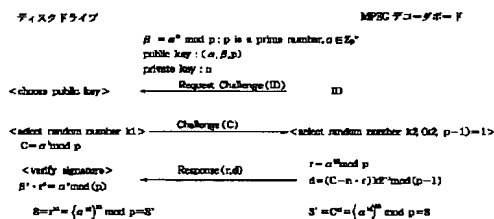
(54) DATA DECODING METHOD AND ITS DEVICE,
AUTHENTICATING METHOD, RECORDING
MEDIUM, DISK PRODUCING METHOD,
RECORDING METHOD AND RECORDING
DEVICE

COPYRIGHT: (C)1998,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To surely prevent illegal copying by ciphering reproduction data which is supplied to a decoder through the use of an undecipherable cipher key.

SOLUTION: When identification data transmitted from an MPEG decoder board and a public key corresponding to its ID are judged to be effective, a disk drive calculates Challenge (C) from an expression $C = \alpha k_1 \bmod p$ and supplies it to the MPEG decoder board. In the expression, α and p are the public keys, p is prime number, and k_1 is a properly selected random value. The MPEG decoder board selects the random value k_2 , calculates digital signature r and d and supplies them to the disk drive. The disk drive calculates $\beta^r \cdot \gamma^d$, calculates $\alpha^c \bmod (p)$, judges whether or not the both values are equal and calculates Session key (S) in the case of being equal. In the meantime, the decoder board calculates Session key (S'). S becomes the value equal to S' and it means the same cipher key is obtained.



(51)Int.Cl. ⁶	識別記号	序内整理番号	F I	技術表示箇所
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 C
G 1 1 B 20/14	3 4 1	9463-5D	G 1 1 B 20/14	3 4 1 B
H 0 4 L 9/14			H 0 4 L 9/00	6 0 1 E
				6 4 1
H 0 4 N 7/24				6 7 5 A

審査請求 未請求 請求項の数23 O L (全 19 頁) 最終頁に続く

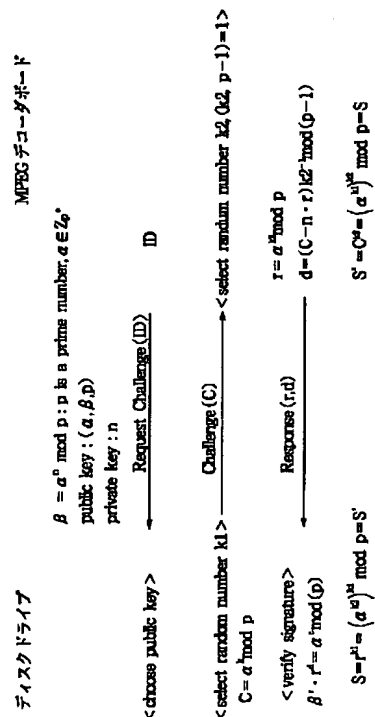
(21)出願番号	特願平9-82598	(71)出願人	000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22)出願日	平成9年(1997)4月1日	(72)発明者	石黒 隆二 東京都品川区北品川6丁目7番35号 ソニ ー株式会社内
(31)優先権主張番号	特願平8-78647	(72)発明者	大澤 義知 東京都品川区北品川6丁目7番35号 ソニ ー株式会社内
(32)優先日	平8(1996)4月1日	(74)代理人	弁理士 稲本 義雄
(33)優先権主張国	日本 (J P)		
(31)優先権主張番号	特願平8-147272		
(32)優先日	平8(1996)6月10日		
(33)優先権主張国	日本 (J P)		

(54)【発明の名称】 データ復号方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置

(57)【要約】

【課題】 より安全な復号化方法を実現する。

【解決手段】 MPEGデコーダボードは、メモリに記憶されているIDをディスクドライブに出力する。ディスクドライブは、DVD-ROMに記憶されているキーテーブルからIDに対応する公開鍵を読み出し、この公開鍵を用いて、Challenge (C)を演算し、MPEGデコーダボードに出力する。MPEGデコーダボードは、Challenge (C)を用いて、デジタルシグニチャ、dを演算し、ディスクドライブに出力する。ディスクドライブは、デジタルシグニチャ、dを用いて、暗号化鍵を演算する。また、MPEGデコーダボードは、Challenge (C)を用いて、暗号化鍵を演算する。



【特許請求の範囲】

【請求項1】 所定の暗号化鍵Sを用いてデータを暗号化することにより得られた暗号化データを第1の装置から受信し、その暗号化データを前記所定の暗号化鍵Sを用いて復号する第2の装置のデータ復号方法において、前記所定の暗号化鍵Sを用いて暗号化された暗号化データを前記第1の装置から受信するステップと、
所定の方法により生成された前記所定の暗号化鍵Sを用いて、前記暗号化データを復号するステップとを備え、
前記所定の暗号化鍵Sを生成する前記所定の方法においては、

前記第1の装置と前記第2の装置のうちの一方が、前記第1の装置と前記第2の装置のうちの他方からの識別データを受信して、前記識別データに対応する公開鍵 α 、 p を選択し、ランダム値 k_1 と前記公開鍵 α 、 p から、 $C = \alpha k_1 \bmod p$

に従って第1のデータCを演算し、その第1のデータCを他方に供給し、

前記他方が、前記公開鍵 α 、 p と、ランダム値 k_2 を用いて第2のデータrを演算して、前記一方に供給するとともに、前記第1のデータCと前記ランダム値 k_2 を用いて前記暗号化鍵Sを演算し、

さらに、前記一方が、前記他方から供給される前記第2のデータrと前記ランダム値 k_1 を用いて前記暗号化鍵Sを演算することを特徴とするデータ復号方法。

【請求項2】 前記第1の装置と前記第2の装置との間で認証が行われ、前記認証においては、

前記他方が、前記第1のデータC、前記第2のデータr、前記公開鍵 p 、前記ランダム値 k_2 および秘密鍵 n を用いて、第3のデータdを演算して、前記一方に供給し、

前記一方が、前記他方から供給される前記第2データrと前記第3のデータdと所定の公開鍵 β とを用いて演算される値と、前記公開鍵 α 、 p と前記第1のデータCを用いて演算される値とを比較することを特徴とする請求項1に記載のデータ復号方法。

【請求項3】 前記データは暗号化鍵Qを用いて暗号化されたデータであり、

前記第2の装置は、前記暗号化鍵Sを用いて前記データを暗号化することにより得られた、暗号化データ及び前記暗号化された暗号化鍵 x 、 y を前記第1の装置から受信し、

前記所定の暗号化鍵Sを用いて前記暗号化データを復号して前記データを生成し、

前記暗号化された暗号化鍵 x 、 y を復号して復号された暗号化鍵Qを生成し、

その復号された暗号化鍵Qを用いて前記データを復号し、

前記暗号化された暗号化鍵 x 、 y は、前記暗号化鍵Qを前記公開鍵 α 、 β 、 p を用いて暗号化することにより得

られた鍵であり、

前記暗号化された暗号化鍵 x 、 y は、秘密鍵 n 及び公開鍵 p を用いて暗号化鍵Qに復号されることを特徴とする請求項2に記載のデータ復号方法。

【請求項4】 前記公開鍵 α 、 p は記録媒体から再生されたデータであることを特徴とする請求項1に記載のデータ復号方法。

【請求項5】 所定の暗号化鍵Sを用いてデータを暗号化することにより得られた暗号化データを第1の装置から受信し、その暗号化データを前記所定の暗号化鍵Sを用いて復号するデータ復号装置において、

前記所定の暗号化鍵Sを用いて暗号化された暗号化データを前記第1の装置から受信する受信手段と、

前記所定の暗号化鍵Sを用いて、前記暗号化データを復号する第1の復号手段とを備え、

さらに、前記所定の暗号化鍵Sを生成するために、

前記第1の装置と前記復号装置のうちの一方が、前記第1の装置と前記復号装置のうちの他方からの識別データを受信して、前記識別データに対応する公開鍵 α 、 p を選択し、ランダム値 k_1 と前記公開鍵 α 、 p から、 $C = \alpha k_1 \bmod p$

に従って、第1のデータCを演算し、その第1のデータCを他方に供給する手段と、

前記他方が、前記公開鍵 α 、 p と、ランダム値 k_2 を用いて第2のデータrを演算して、前記一方に供給するとともに、前記第1のデータCと前記ランダム値 k_2 を用いて前記暗号化鍵Sを演算する手段と、

さらに、前記一方が、前記他方から供給される前記第2のデータrと前記ランダム値 k_1 を用いて前記暗号化鍵Sを演算する手段とを備えることを特徴とするデータ復号装置。

【請求項6】 前記第1の装置と前記データ復号装置との間で認証が行われ、前記認証のために、

前記他方が、前記第1のデータC、前記第2のデータr、前記公開鍵 p 、前記ランダム値 k_2 および秘密鍵 n を用いて、第3のデータdを演算して、前記一方に供給する手段と、

前記一方が、前記他方から供給される前記第2のデータrと前記第3のデータdと所定の公開鍵 β とを用いて演算される値と、前記公開鍵 α 、 p と前記第1のデータCを用いて演算される値とを比較する手段とを備えることを特徴とする請求項5に記載のデータ復号装置。

【請求項7】 前記データは暗号化鍵Qを用いて暗号化されたデータであり、

前記復号装置は、

前記暗号化鍵Sを用いて前記データを暗号化することにより得られた、暗号化データ及び前記暗号化された暗号化鍵 x 、 y を前記第1の装置から受信する受信手段と、前記所定の暗号化鍵Sを用いて前記暗号化データを復号して前記データを生成する第1の復号手段と、

前記暗号化された暗号化鍵 x 、 y を復号して復号された暗号化鍵 Q を生成する鍵復号手段と、

その復号された暗号化鍵 Q を用いて前記データを復号する第 2 の復号手段とを有し、

前記暗号化された暗号化鍵 x 、 y は、前記暗号化鍵 Q を前記公開鍵 α 、 β 、 p を用いて暗号化することにより得られた鍵であり、

前記暗号化された暗号化鍵 x 、 y は、秘密鍵 n 及び公開鍵 p を用いて暗号化鍵 Q に復号されることを特徴とする請求項 5 に記載のデータ復号装置。

【請求項 8】 前記公開鍵 α 、 p は記録媒体から再生されたデータであることを特徴とする請求項 5 に記載のデータ復号装置。

【請求項 9】 所定の暗号化鍵 S を用いてデータを暗号化して、暗号化データを出力する第 1 の装置と、前記暗号化データを受信して、前記所定の暗号化鍵 S を用いて前記暗号化データを復号するデータ復号装置との間で、前記第 1 の装置と前記データ復号装置の一方が他方を認証する認証方法において、

前記第 1 の装置と前記データ復号装置のうちの一方が、前記第 1 の装置と前記データ復号装置のうちの他方からの識別データを受信して、前記識別データに対応する公開鍵 α 、 p を選択し、ランダム値 k_1 と前記公開鍵 α 、 p から、

$$C = \alpha k_1 \bmod p$$

に従って、第 1 のデータ C を演算し、その第 1 のデータ C を他方に供給するステップと、

前記他方が、前記公開鍵 α 、 p と、ランダム値 k_2 を用いて第 2 のデータ r 、 d を演算して、前記一方に供給するステップと、

前記一方が、前記他方から供給される前記第 2 のデータ r 、 d と所定の公開鍵 β とを用いて演算される値と、前記公開鍵 α 、 p と前記第 1 のデータ C を用いて演算される値とを比較するステップとを備えることを特徴とする認証方法。

【請求項 10】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体において、

前記記録媒体は記録データを含んでおり、前記記録データは、

前記暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、

前記データと前記キーテーブルを記録するステップから生成されていることを特徴とする記録媒体。

【請求項 11】 前記キーテーブルには、前記第 1 の装置または前記データ復号装置を識別するとき用いられる

公開鍵 β が、さらに、前記識別データに対応して含まれていることを特徴とする請求項 10 に記載の記録媒体。

【請求項 12】 前記データは暗号化鍵 Q により暗号化されたデータであり、

前記キーテーブルには、前記暗号化鍵 Q を前記公開鍵 α 、 β 、 p を用いて暗号化した暗号化鍵 x 、 y が、さらに前記識別データに対応して含まれていることを特徴とする請求項 10 に記載の記録媒体。

【請求項 13】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録方法において、

前記暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、

前記データと前記キーテーブルを記録するステップとを備えることを特徴とする記録方法。

【請求項 14】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録装置において、

前記暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成する生成手段と、

前記データと前記キーテーブルを記録する記録手段とを備えることを特徴とする記録装置。

【請求項 15】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体において、

前記記録媒体は記録データを含んでおり、前記記録データは、

前記第 1 の装置または前記データ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルを生成するステップと、

前記データと前記キーテーブルを記録するステップとから生成されていることを特徴とする記録媒体。

【請求項 16】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録方法において、

前記第1の装置または前記データ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成するステップと、前記データと前記キーテーブルを記録するステップとを備えることを特徴とする記録方法。

【請求項17】 データを所定の暗号化鍵Sを用いて暗号化して、暗号化データを出力する第1の装置と、前記第1の装置からの前記暗号化データを前記暗号化鍵Sを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録装置において、

前記第1の装置または前記データ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成する生成手段と、前記データと前記キーテーブルを記録する記録手段とを備えることを特徴とする記録装置。

【請求項18】 暗号化鍵Qで暗号化されたデータを所定の暗号化鍵Sを用いて暗号化して、暗号化データを出力する第1の装置と、前記第1の装置からの前記暗号化データを前記暗号化鍵Sを用いて復号し、さらに、暗号化鍵Qを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体において、前記記録媒体は記録データを含んでおり、前記記録データは、

データを暗号化鍵Qで暗号化して、暗号化鍵Qで暗号化されたデータを生成するステップと、前記暗号化鍵Qを、前記暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p と、前記第1の装置または前記データ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を前記第1の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと前記暗号化鍵Qで暗号化されたデータと前記キーテーブルを記録するステップとから生成されていることを特徴とする記録媒体。

【請求項19】 暗号化鍵Qで暗号化されたデータを所定の暗号化鍵Sを用いて暗号化して、暗号化データを出力する第1の装置と、前記第1の装置からの前記暗号化データを前記暗号化鍵Sを用いて復号し、さらに、暗号化鍵Qを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録方法において、

データを暗号化鍵Qで暗号化して、暗号化鍵Qで暗号化されたデータを生成するステップと、前記暗号化鍵Qを、前記暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p と、前記第1の装置または前記データ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を前記第1の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと

前記暗号化鍵Qで暗号化されたデータと前記キーテーブルを記録するステップとを備えることを特徴とする記録方法。

【請求項20】 暗号化鍵Qで暗号化されたデータを所定の暗号化鍵Sを用いて暗号化して、暗号化データを出力する第1の装置と、前記第1の装置からの前記暗号化データを前記暗号化鍵Sを用いて復号し、さらに、暗号化鍵Qを用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録装置において、

データを暗号化鍵Qで暗号化して、暗号化鍵Qで暗号化されたデータを生成する暗号化手段と、前記暗号化鍵Qを、前記暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p と、前記第1の装置または前記データ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を前記第1の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成する生成手段と前記暗号化鍵Qで暗号化されたデータと前記キーテーブルを記録する記録手段とを備えることを特徴とする記録装置。

【請求項21】 データを所定の暗号化鍵Sを用いて暗号化して、暗号化データを出力する第1の装置と、前記第1の装置からの前記暗号化データを前記暗号化鍵Sを用いて復号するデータ復号装置とにより構成される再生装置によって再生されるディスクを製造するためのディスク製造方法において、

前記暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p を前記第1の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、前記データと前記キーテーブルを原盤に記録するステップと、前記原盤から前記ディスクを生成するステップとを備えることを特徴とするディスク製造方法。

【請求項22】 データを所定の暗号化鍵Sを用いて暗号化して、暗号化データを出力する第1の装置と、前記第1の装置からの前記暗号化データを前記暗号化鍵Sを用いて復号するデータ復号装置とにより構成される再生装置によって再生されるディスクを製造するためのディスク製造方法において、

前記第1の装置または前記データ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成するステップと、前記データと前記キーテーブルを原盤に記録するステップと、前記原盤から前記ディスクを生成するステップとを備えることを特徴とするディスク製造方法。

【請求項23】 暗号化鍵Qで暗号化されたデータを所定の暗号化鍵Sを用いて暗号化して、暗号化データを出力

する第1の装置と、前記第1の装置からの前記暗号化データを前記暗号化鍵Sを用いて復号し、さらに、暗号化鍵Qを用いて復号するデータ復号装置とにより構成される再生装置によって再生されるディスクを製造するためのディスク製造方法において、データを暗号化鍵Qで暗号化して、暗号化鍵Qで暗号化されたデータを生成するステップと、前記暗号化鍵Qを、前記暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p と、前記第1の装置または前記データ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を前記第1の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、前記暗号化鍵Qで暗号化されたデータと前記キーテーブルを原盤に記録するステップと、前記原盤から前記ディスクを生成するステップとを備えることを特徴とするディスク製造方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データ復号方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置に関し、特に暗号化されているデータを、より安全に復号することができるようにした、データ復号化方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置に関する。

【0002】

【従来の技術】最近、デジタルビデオディスク（以下、DVDと記載する）のフォーマットが統一化されつつあり、統一化された場合、従来のアナログのビデオディスクに代わって普及することが期待されている。このDVDにおいては、より長時間のビデオデータを記録することができるようにするために、ビデオデータが圧縮符号化（例えば、MPEG（Moving Picture Expert Group）方式、以下、MPEGと記載し、MPEG方式を用いて説明する）されて記録される。従って、再生時には、再生データを復号する必要がある。

【0003】ところで、DVDにおいては、ビデオデータがデジタル的に記録されているため、これを他の記録媒体にコピーすると、ほとんどオリジナルのDVDと遜色のない再生画像が得られる記録媒体を大量に複製することが可能となる。つまり、ディスクドライブとMPEGデコーダとの間でのデータの授受を盗聴され、この盗聴されたデータから不正のスタンパを生成することにより、不正のディスクが大量に複製されることになる。また、不正に製造されたMPEGデコーダを使用して、ディスクドライブからの再生データを復号し、この不正に復号された不正のスタンパを生成することにより、不正のディスクが大量に複製されることになる。

【0004】このような不正コピーを防止したり、不正に製造されたMPEGデコーダを排除するために、ディスクドライブとMPEGデコーダとの間のデータとの授受において、正規のMPEGデコーダであるか否かを認証し、正規のMPEGデコーダであると認証された場合、ディスクドライブから再生データを暗号化鍵を用いて暗号化して、暗号化データをMPEGデコーダに供給する。そして、MPEGデコーダは、この暗号化データを暗号化鍵を用いて復号（解読）し、さらに、復号（解読）された符号化データを復号するようにすることが考えられている。

【0005】したがって、このような対策を取ることで、不正に製造されたMPEGデコーダである場合は、ディスクドライブからの再生データがMPEGデコーダに供給されず、不正コピーを防止でき、かつ不正に製造されたMPEGデコーダを排除することができる。また、仮に正規のMPEGデコーダを装ってディスクドライブにアクセスされた場合、もしくはディスクドライブとMPEGデコーダとの間でのデータの授受を盗聴された場合に、ディスクドライブからの再生データを得られたとしても、その再生データは暗号化されているため、そのままではそのデータを用いることができない。従って、実質的なコピーを防止することができる。

【0006】

【発明が解決しようとする課題】しかしながら、従来より提案されている単純な暗号化鍵を用いてMPEGデコーダに供給する再生データを暗号化し、MPEGデコーダにおいて、その暗号化された再生データを復号する方法は、暗号化鍵が破られ易いという課題があった。

【0007】本発明はこのような状況に鑑みてなされたものであり、本発明の目的は、デコーダに供給する再生データを破られ難い暗号化鍵を用いて暗号化することにより、不正コピーを確実に防止することができるようにすることにある。

【0008】また、本発明の他の目的は、ディスクドライブからの再生データを暗号化する暗号化鍵の管理を容易にすることができるようにすることにある。

【0009】

【課題を解決するための手段】請求項1に記載のデータ復号方法は、所定の暗号化鍵Sを用いて暗号化された暗号化データを第1の装置から受信するステップと、所定の方法により生成された所定の暗号化鍵Sを用いて、暗号化データを復号するステップとを備え、所定の暗号化鍵Sを生成する所定の方法においては、第1の装置と第2の装置のうち的一方が、第1の装置と第2の装置のうちの他方からの識別データを受信して、識別データに対応する公開鍵 α 、 p を選択し、ランダム値 k_1 と公開鍵 α 、 p から、 $C = \alpha k_1 \bmod p$ に従って第1のデータCを演算し、その第1のデータCを他方に供給し、他方が、公開鍵 α 、 p と、ランダム値 k_2 を用いて第2のデ

ータ r を演算して、一方に供給するとともに、第1のデータ C とランダム値 k_2 を用いて暗号化鍵 S を演算し、さらに、一方が、他方から供給される第2のデータ r とランダム値 k_1 を用いて暗号化鍵 S を演算することを特徴とする。

【0010】請求項5に記載のデータ復号装置は、所定の暗号化鍵 S を用いて暗号化された暗号化データを第1の装置から受信する受信手段と、所定の暗号化鍵 S を用いて、暗号化データを復号する第1の復号手段とを備え、さらに、所定の暗号化鍵 S を生成するために、第1の装置と復号装置のうちの一方が、第1の装置と復号装置のうちの他方からの識別データを受信して、識別データに対応する公開鍵 α 、 p を選択し、ランダム値 k_1 と公開鍵 α 、 p から、 $C = \alpha k_1 \bmod p$ に従って、第1のデータ C を演算し、その第1のデータ C を他方に供給する手段と、他方が、公開鍵 α 、 p と、ランダム値 k_2 を用いて第2のデータ r を演算して、一方に供給するとともに、第1のデータ C とランダム値 k_2 を用いて暗号化鍵 S を演算する手段と、さらに、一方が、他方から供給される第2のデータ r とランダム値 k_1 を用いて暗号化鍵 S を演算する手段とを備えることを特徴とする。

【0011】請求項9に記載の認証方法は、第1の装置とデータ復号装置のうちの一方が、第1の装置とデータ復号装置のうちの他方からの識別データを受信して、識別データに対応する公開鍵 α 、 p を選択し、ランダム値 k_1 と公開鍵 α 、 p から、 $C = \alpha k_1 \bmod p$ に従って、第1のデータ C を演算し、その第1のデータ C を他方に供給するステップと、他方が、公開鍵 α 、 p と、ランダム値 k_2 を用いて第2のデータ r 、 d を演算して、一方に供給するステップと、一方が、他方から供給される第2のデータ r 、 d と所定の公開鍵 β とを用いて演算される値と、公開鍵 α 、 p と第1のデータ C を用いて演算される値とを比較するステップとを備えることを特徴とする。

【0012】請求項10に記載の記録媒体は、記録媒体は記録データを含んでおり、記録データは、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を第1の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、データとキーテーブルを記録するステップから生成されていることを特徴とする。

【0013】請求項13に記載の記録方法は、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を第1の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを記録するステップとを備えることを特徴とする。

【0014】請求項14に記載の記録装置は、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を第1の装置またはデータ復号装置を識別する識別データに対応させ

ることにより、キーテーブルデータを生成する生成手段と、データとキーテーブルを記録する記録手段とを備えることを特徴とする。

【0015】請求項15に記載の記録媒体は、記録媒体は記録データを含んでおり、記録データは、第1の装置またはデータ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルを生成するステップと、データとキーテーブルを記録するステップとから生成されていることを特徴とする。

【0016】請求項16に記載の記録方法は、第1の装置またはデータ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを記録するステップとを備えることを特徴とする。

【0017】請求項17に記載の記録装置は、第1の装置またはデータ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成する生成手段と、データとキーテーブルを記録する記録手段とを備えることを特徴とする。

【0018】請求項18に記載の記録媒体は、記録媒体は記録データを含んでおり、記録データは、データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成するステップと、暗号化鍵 Q を、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、第1の装置またはデータ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を第1の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと暗号化鍵 Q で暗号化されたデータとキーテーブルを記録するステップとから生成されていることを特徴とする。

【0019】請求項19に記載の記録方法は、データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成するステップと、暗号化鍵 Q を、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、第1の装置またはデータ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を第1の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと暗号化鍵 Q で暗号化されたデータとキーテーブルを記録するステップとを備えることを特徴とする。

【0020】請求項20に記載の記録装置は、データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成する暗号化手段と、暗号化鍵 Q を、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、第1の装置またはデータ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を第1の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成する生成手段と暗号化鍵 Q で暗号化されたデータとキーテーブルを記録する記録手段とを備えることを特徴とする。

【0021】請求項21に記載のディスク製造方法は、暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p を第1の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを原盤に記録するステップと、原盤からディスクを生成するステップとを備えることを特徴とする。

【0022】請求項22に記載のディスク製造方法は、第1の装置またはデータ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを原盤に記録するステップと、原盤からディスクを生成するステップとを備えることを特徴とする。

【0023】請求項23に記載のディスク製造方法は、データを暗号化鍵Qで暗号化して、暗号化鍵Qで暗号化されたデータを生成するステップと、暗号化鍵Qを、暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p と、第1の装置またはデータ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を第1の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、暗号化鍵Qで暗号化されたデータとキーテーブルを原盤に記録するステップと、原盤からディスクを生成するステップとを備えることを特徴とする。

【0024】

【発明の実施の形態】図1は、本発明を適用した第1の実施の形態のパーソナルコンピュータの構成例を示している。この第1の実施の形態において、パーソナルコンピュータ1は、ROMタイプのデジタルビデオディスク（以下、DVD-ROMと記載する）2を駆動するディスクドライブ11と、ディスクドライブ11によって再生された再生データが供給され、この再生データをデコードするMPEGデコーダボード12とから構成されている。MPEGデコーダボード12からの復号された画像データ（以下、コンテンツデータ（Contents）と記載する）は、モニタ3に供給され、モニタ3は図示しない表示画面に再生画像を表示するようになされている。

【0025】ディスクドライブ11は、DVD-ROM2を駆動し、所定のアクセス点にアクセスすることにより、そこに記録されているデータを再生する駆動部21、駆動部21からの再生データを暗号化し、その暗号化データを出力する暗号化部22、および、駆動部21と暗号化部22を制御する制御部20から構成されている。DVD-ROM2には、所定の位置（例えば最内周トラック）に、暗号化に使用される公開鍵 α 、 β 、 p を含むキーテーブルのデータが予め記録されている。なお、DVD-ROM2に記録されているコンテンツデータは、MPEG方式によって符号化されているデータである。

【0026】また、MPEGデコーダボード12は、パ

ーソナルコンピュータ1に対して、適宜装着されるボードであって、暗号化部22より供給される暗号化データを復号（解読）し、復号（解読）された再生データを出力する復号部31を有している。この復号部31は、復号（解読）処理を行うのに必要な秘密鍵 n と、MPEGデコーダボード12を識別するIDを記憶するメモリ33を有している。

【0027】復号部31より出力された復号（解読）された再生データは、MPEGデコード部32に供給され、MPEGデコード部32は、MPEG方式に従って復号（解読）された再生データを復号し、コンテンツデータとして出力するようになされている。制御部30は、復号部31とMPEGデコード部32を制御するようになされている。

【0028】次に、図2と図3のフローチャート、図4のタイミングチャート及び図5の模式図を参照して、図1の第1の実施の形態の動作について説明する。なお、図2は、ディスクドライブ11の動作を説明するためのフローチャートであり、図3は、MPEGデコーダボード12の動作を説明するフローチャートである。また、図4のタイミングチャートは、ディスクドライブ11とMPEGデコーダボード12との間において授受されるデータと、各データに対応して実行される演算を表している。さらに、図5は、ディスクドライブ11とMPEGデコーダボード82との間でのデータの流れを示すための模式図である。

【0029】DVD-ROM2に記録されているデータを再生する場合、最初に、図3のステップS21において、MPEGデコーダボード12の制御部30は、MPEGデコーダボード12の識別データとしてのIDを復号部31のメモリ33から読み出し、ディスクドライブ11の制御部20に送信する。このIDは、図4に示すように、Request Challenge（ID）として、ディスクドライブ11に送られる。

【0030】図2のステップS1において、ディスクドライブ11の制御部20は、MPEGデコーダボード12の制御部30から送られてきたIDを受け取る。そして、制御部20はステップS2に進み、ステップS1で受け取ったIDに対応する公開鍵を、DVD-ROM2から読み取るように、駆動部20を制御する。

【0031】すなわち、図5に模式的に示すように、DVD-ROM2の所定のトラックには、キーテーブルとして、このDVD-ROM2を再生して得られるMPEG方式によって符号化されているコンテンツデータを暗号化する複数の公開鍵（public key）が、各公開鍵（key1, key2, key3, ...）が有効であるか否かを表すフラグと共に記録されている。図5において、有効な公開鍵（key1, key2）は○印を付して表し、無効な公開鍵（key3）は×印を付して表している。DVD-ROM2を初めて製造したとき、全て

の公開鍵は有効とされている。しかしながら、例えば、公開鍵の中の所定のもの（図5の第1の実施の形態の場合、key 3）が第3者に破られてしまったような場合、その公開鍵に対応するフラグは、以後、無効として記録される。

【0032】なお、各公開鍵key 1, key 2, key 3, ...は、それぞれ公開鍵($\alpha 1$, $\beta 1$, $p 1$), ($\alpha 2$, $\beta 2$, $p 2$), ($\alpha 3$, $\beta 3$, $p 3$), ...で構成される。

【0033】このような公開鍵と有効フラグを表すキーテーブルが、DVD-ROM2のROM領域に記録されている場合においては、これを書き換えることができないため、新しいバージョンのディスクとして、実質的に同一のコンテンツデータが記録されているディスクを新たに製造するとき、キーテーブルの有効フラグだけが書き換えられる。

【0034】制御部20は、駆動部21を制御し、駆動部21は、DVD-ROM2の所定のトラックに記録されているキーテーブルを読み出す。そして、この読み出したキーテーブルは制御部20に供給され、制御部20は、この読み出されたキーテーブルから、ステップS1で受け取ったIDに対応する公開鍵及びその公開鍵に対応するフラグを検出する。換言すれば、MPEGデコーダボード12の正規の製造者に対してはIDが予め与えられており、DVD-ROM2の製造者は、各IDに対応する公開鍵を選定し、テーブルに記憶しておく。そこで、このステップS2で、各IDに対応する公開鍵及びフラグが検出される。

【0035】さらに、ステップS3において、制御部20は、その公開鍵に対応するフラグが有効とされているか否かを判定する。上述したように、例えば、不正コピーを行っているMPEGデコーダボード12の製造者（ボードメーカー）に割り当てられているIDが発見された場合においては、そのIDに対応する公開鍵は無効とされる。そして、その発見後に製造されるDVD-ROM2には、その公開鍵を無効とするフラグが記録される。ステップS1で受け取ったIDに対応する公開鍵が無効と判定された場合、処理が終了される。すなわち、この場合においては、MPEGデコーダボード12は、DVD-ROM2の再生データを受け取ることができないことになる。

【0036】一方、ステップ3において、ステップS1で受け取ったIDに対応する公開鍵が有効であると判定された場合、ステップS4に進み、制御部20は、次式(1)からChallenge (C)を計算し、図4に示すように、このChallenge (C)としてMPEGデコーダボード12の制御部30に供給する。

$$C = \alpha k1 \bmod p \cdots (1)$$

【0037】ここで、 α , p は、DVD-ROM2のキーテーブルに記録されている公開鍵であり、 p は素数で

ある。また、 $k1$ は、適宜選択されるランダムな番号（値）である。また、 $A \bmod B$ は、 A を B で割算したとき得られる剰余を表している。

【0038】上述した式(1)は、トラップドア関数（離散対数問題）として知られており、 $k1$ から C は容易に計算できるが、 C から $k1$ を計算することができる関数は知られていない。

【0039】図4に示すように、このようにして計算されたChallenge (C)は、MPEGデコーダボード12の制御部30に供給される。制御部30は、図3のステップS22において、このChallenge (C)を受け取る。そして、制御部30は、ステップS23に進み、所定のランダムな番号 $k2$ を選択し、次式(2)、(3)からデジタルシグニチャ r , d を演算し、その結果をResponse (r , d)として、ディスクドライブ11に供給する。

$$r = \alpha k2 \bmod p \cdots (2)$$

$$d = (C - n \cdot r) k2^{-1} \bmod (p - 1) \cdots (3)$$

【0040】なお、このランダムな値 $k2$ は、 $p - 1$ と素の関係にある。

【0041】図4に示すように、上述した式(2)及び(3)から求められたデジタルシグニチャ r , d は、Response (r , d)として、ディスクドライブ11の制御回路20に供給される。制御部20は、図2のステップS5において、このResponse (r , d)を受け取り、ステップS6に進み、ステップ6において、このResponse (r , d)内のデジタルシグニチャ r , d をチェックする。

【0042】すなわち、制御部20は、図4に示すように、 $\beta r \cdot r d$ を演算するとともに、 $\alpha C \bmod (p)$ を演算し、両者の値が等しいか否かを判定する。MPEGデコーダボード12が、正規のデコーダである場合、デジタルシグニチャ r , d と公開鍵 β とを用いて演算される値 $\beta r \cdot r d$ の値は、Challenge (C)、公開鍵 α , p を用いて求められる値 $\alpha C \bmod (p)$ の値と等しくなる。この2つの演算値が等しくなることは、ElGamal Signature Schemeとして、よく知られている(A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 21 (1985), 469-472)。逆に、MPEGデコーダボード12が正規のデコーダではない場合、両者の値は異なるものとなる。この場合、処理は終了される。従って、この場合、DVD-ROM2の再生データはMPEGデコーダボード12に出力されないことになる。なお、ここまでのデータの授受の流れが、図5に示されるKey Exchangeに対応している。

【0043】ステップS6において、演算された2つの値が等しいと判定された場合、ステップS7に進み、制御部20は、Session key (S)を次式(4)より演算す

る (図5のSession Key S)。

$S = rkl \cdots (4)$

【0044】一方、MPEGデコーダボード12の制御部30は、図3のステップS23において、Response (r, d) を計算して、ディスクドライブ11に供給した後、ステップS24に進み、ステップS22で受け取ったChallenge (C) を用いて次式 (5) に従って、Session key (S*) を演算する (図5のSession Key S*)。

$$S' = Ck2 \cdots (5)$$

【0045】図2のフローチャートのステップS7において、ディスクドライブ11の制御部20によって計算されたSession Key Sと、図3のフローチャートのステップS24においてMPEGデコーダボード12の制御部30によって演算されたSession Key S' は、それぞれ次式 (6) 及び (7) で表され、両者は等しい値となる。すなわち、ディスクドライブ11とMPEGデコーダボード12において、それぞれ同一の暗号化鍵が得られたことになる。

$S = rkl = (\alpha k2) k1 \bmod p \cdots (6)$

$S' = Ck2 = (\alpha k1) k2 \bmod p \cdots (7)$

【0046】このことは、Diffie-Hellman Key Exchangeにおいて知られている (Diffie-Hellman W. Diffie and M. E. Hellman. Multiuser cryptographic techniques. A FIPS Conference Proceedings, 45 (1976), 102-112)。

【0047】そこで、ディスクドライブ11の制御部20は、ステップS8に進み、駆動部21にDVD-ROM2を駆動させるとともに、ステップS7で求めたSession Key Sを暗号化部22に供給する。そして、駆動部21は、DVD-ROM2の所定の位置から記録されているデータを再生する。暗号化部22は、駆動部21でDVD-ROM2から再生された再生データをステップS7で求めたSession Key Sを用いて暗号化して、暗号化データを生成する。そして、この暗号化データは、MPEGデコーダボード12に供給される (図5のEncryption)。

【0048】MPEGデコーダボード12の復号部31は、図3のステップS25で、暗号化部22から供給された暗号化データを受け取り、ステップS26において、その暗号化データを、ステップS24で求めたSession Key S' を用いて復号 (解読) する (図5のDecryption)。上述したように、Session Key S' は、セッションキーSと同一の値であるので、正しい復号 (解読) を行うことができる。そして、この復号 (解読) された再生データ (符号化されているコンテンツデータ) がMPEGデコード部32に供給される。

【0049】MPEGデコード部32は、復号部31によって復号 (解読) された符号化されているコンテンツデータを受け取り、MPEG方式で符号化されているその復号 (解読) されたコンテンツデータを復号し、この

復号されたコンテンツデータをモニタ3に供給する (図5のDecode)。そして、モニタ3は、このコンテンツデータを再生画像として図示しない表示画面に表示する。

【0050】上述したように、第1の実施の形態においては、公開鍵を使用し、この公開鍵をディスクに記録しておく、公開鍵の配布が容易となる。また、公開鍵を複数記録しておけば、MPEGデコーダボード12の製造者 (ボードメーカー) に秘密鍵を配布するとき、ボードメーカー毎に異なる鍵を割り当てることができる。よって、1つのボードメーカーの秘密鍵が破られた場合でも、他のボードメーカーには別の秘密鍵が割り当てられているため、他のボードメーカーの秘密鍵はそのまま使用でき、被害を最小限に食い止めることができる。

【0051】さらに、ディスクドライブ11において、秘密鍵nはもとより、公開鍵 α , β , pを保持しておく必要がないので、ディスクドライブにおける管理が容易となる。

【0052】なお、ディスクドライブ内の制御部20は、暗号化部22と一体化して構成してもよい。また、MPEGデコーダボード内の制御部30は、復号部31と一体化して構成してもよい。

【0053】また、以上の第1の実施の形態においては、MPEGデコーダボード12からIDをディスクドライブ11に供給し、ディスクドライブ11において認証を行うようにしたが、ディスクドライブ11からIDを供給し、MPEGデコーダボード12において認証を行うようにしてもよい。また、ディスクとして、DVD-ROMを用いる場合を例としたが、本発明は、その他の記録媒体に記録されているデータを再生する場合にも適用することができる。なお、ディスクがRAMタイプのディスクである場合、制御部20は、所定の指令が入力されたとき、そのフラグを無効なフラグに書き換えることも可能である。

【0054】図6は、以上の第1の実施の形態におけるDVD-ROM2に対してデータを記録する記録装置の構成例を示している。図6に示すように、合成部51は、ID供給源41からのID、フラグ供給源42からのフラグ、および公開鍵供給源43からの公開鍵 α , β , pをキーテーブル (Key Table) のデータとして合成し、その合成されたデータを合成部52に供給する。また、コンテンツデータ供給源44からのビデオデータ等のコンテンツデータ (Contents) がMPEGエンコード部53に供給され、MPEGエンコード部53は、コンテンツデータをMPEG方式に従って符号化し、符号化されたコンテンツデータを合成部52に供給する。合成部52は、合成部51より入力されたキーテーブルのデータと、MPEGエンコード部53からの符号化されたコンテンツデータを合成して、記録データとして出力する。そして、この記録データが原盤54に記録される。さらに、その原盤54から大量のレプリカとしての

DVD-ROM2が生成される。これにより、DVD-ROM2には、コンテンツデータの他、各IDに対応したフラグ及び公開鍵からなるキーテーブルが記録される。

【0055】次に、本発明を適用した第2の実施の形態について説明する。なお、第2の実施の形態を説明するにあたり、まず、コンテンツデータをDVD-ROMに記録する記録装置を説明した後、パーソナルコンピュータの構成を説明する。

【0056】図7は、第2の実施の形態におけるDVD-ROM72に対してデータを記録する記録装置の構成例を示している。この第2の実施の形態においては、コンテンツデータが暗号化され、暗号化コンテンツデータがDVD-ROM72に記録されるようになされている。

【0057】コンテンツ情報源61からのコンテンツデータは、MPEGエンコード部69に供給される。MPEGエンコード部69は、コンテンツデータをMPEG方式に従って符号化し、符号化コンテンツデータを暗号化部62に供給する。また、暗号化鍵供給源63からの暗号化鍵Qが暗号化部62に供給される。暗号化部62は、暗号化鍵Qを用いて、例えば、符号化コンテンツデータをDES (Data Encryption Standard) 方式に従って暗号化し、暗号化コンテンツデータを合成部70に供給する。

【0058】一方、この暗号化鍵Qは、暗号化鍵暗号化部64にも供給される。また、公開鍵供給源67からの公開鍵 α 、 β 、 p が暗号化鍵暗号化部64に供給され、暗号化鍵暗号化部64は、次式(8)及び(9)に従って、公開鍵 α 、 β 、 p を用いて、暗号化鍵Qを暗号化し、暗号化された暗号化鍵 x 、 y を生成する。

$$x = \alpha k_3 \bmod (p) \quad \cdots (8)$$

$$y = Q \cdot \beta k_3 \bmod (p) \quad \cdots (9)$$

ここで、 k_3 は、適宜選択されるランダムな番号(値)である。

【0059】また、合成部68は、ID供給源65からのID、フラグ供給源66からのフラグ、公開鍵供給源67からの公開鍵 α 、 β 、 p 、並びに暗号化部64からの暗号化された暗号化鍵 x 、 y を合成し、キーテーブルとして合成部70に供給する。合成部70は、合成部68から供給されたキーテーブルのデータと、暗号化部62からの暗号化コンテンツデータを合成して、記録データとして出力する。そして、この記録データが原盤71に記録される。さらに、その原盤71から大量のレプリカとしてのDVD-ROM72が製造される。これにより、図7に示すように、DVD-ROM72には、暗号化コンテンツデータの他に、各IDに対応したフラグ、公開鍵 $key_i (\alpha_i, \beta_i, p_i)$ 、並びに暗号化された暗号化鍵(x_i, y_i)が、キーテーブルとして記録される。

【0060】次に、上述したような方法で製造されたDVD-ROM72に記録されているデータを再生する第2の実施の形態のパーソナルコンピュータの構成について説明する。図8は、本発明を適用した第2の実施の形態のパーソナルコンピュータの構成例を示している。パーソナルコンピュータ80は、DVD-ROM72をドライブするディスクドライブ81と、ディスクドライブ81によって再生された再生データが供給され、この再生データをデコードするMPEGデコーダボード82から構成されている。MPEGデコーダボード82からの復号されたコンテンツデータは、モニタ73に供給され、モニタ73は、図示しない表示画面に再生画像を表示するようになされている。この場合におけるディスクドライブ81とMPEGデコーダボード82の構成は、基本的に図1に示す場合と同様である。

【0061】ディスクドライブ81は、DVD-ROM72を駆動し、所定のアクセス点にアクセスして、そこに記録されているデータを再生する駆動部91、駆動部91から再生データを暗号化し、その暗号化データを出力する暗号化部92、及び駆動部91と暗号化部92を制御する制御部90から構成されている。DVD-ROM72には、所定の位置(例えば最内周トラック)に、暗号化に使用される公開鍵 α 、 β 、 p 及び暗号化された暗号化鍵 x 、 y を含むキーテーブルのデータが予め記録されている。なお、DVD-ROM72に記憶されているコンテンツデータは、MPEG方式によって符号化されているデータである。

【0062】また、MPEGデコーダボード82は、第1の実施の形態と同様に、パーソナルコンピュータ80に対して、適宜装着されるボードであって、暗号化部92より供給される暗号化データを復号(解読)し、その復号(解読)された暗号化コンテンツデータを出力する復号部101を有している。この復号部101は、復号(解読)処理を行うために必要な秘密鍵 n と、MPEGデコーダボード82を識別するIDを記憶するメモリ103を有している。

【0063】復号部101から出力された復号された暗号化コンテンツデータは、復号部104に供給される。また、暗号化鍵復号部105は、ディスクドライブ81の駆動部91からの暗号化された暗号化鍵 x 、 y を受け取り、秘密鍵 n と公開鍵 p を用いてこの暗号化鍵Qを復号(解読)し、この復号された暗号化鍵Qを復号鍵として復号部104に供給する。そして復号部104は、この復号鍵を用いて暗号化コンテンツデータを復号(解読)し、復号(解読)された符号化コンテンツデータは、MPEGデコード部102に供給され、MPEG方式によって復号され、コンテンツデータとして出力されるようになされている。制御部100は、復号部101、MPEGデコーダ部102、復号部104及び暗号化鍵復号部105を制御する。

【0064】次に、図9と図10のフローチャート、図11のタイミングチャート、及び図12の模式図を参照して、その動作について説明する。図9は、図8のディスクドライブ81の処理を説明するフローチャートであり、図10は、図8のMPEGデコーダボード82の動作を説明するフローチャートである。また、図11のタイミングチャートは、ディスクドライブ81とMPEGデコーダボード82との間において授受されるデータと、各データに対応して実行される演算を表している。さらに、図12は、ディスクドライブ81とMPEGデコーダボード82との間のデータの流れを示すための模式図である。

【0065】DVD-ROM72に記録されているデータを再生する場合、最初に図10のステップS51において、MPEGデコーダボード82の制御部100は、MPEGデコーダボードの識別データとしてのIDを復号部101のメモリ103から読み出し、ディスクドライブ81の制御部90に送信する。このIDは、図11に示すように、Request Challenge (ID) としてディスクドライブ81に送られる。

【0066】ディスクドライブ81の制御部90は、MPEGデコーダボード82の制御部100から送られてきたIDを図9のステップS31において受け取る。そして、制御部90はステップS32に進み、ステップS31で受け取ったIDに対応する公開鍵を、DVD-ROM72から読み取るように、駆動部91を制御する。

【0067】すなわち、図12に模式的に示されるように、DVD-ROM72の所定のトラックには、キーテーブルとして、コンテンツデータを暗号化した暗号化鍵Qを公開鍵を用いて暗号化した暗号化された暗号化鍵x、yと、このDVD-ROM72を再生して得られるMPEG方式によって符号化されているコンテンツデータを暗号化する公開鍵 (public key) とが、各公開鍵 (key 1, key 2, key 3, ……………) 及び暗号化された暗号化鍵 ((x 1, y 1), (x 2, y 2), (x 3, y 3) ……………) が有効であるか否かを表すフラグと共に記録されている。

【0068】図12において、有効な公開鍵 (key 1, key 2) 及び暗号化された暗号化鍵 ((x 1, y 1), (x 2, y 2)) は○印を付して表し、無効な公開鍵 (key 3) 及び暗号化された暗号化鍵 (x 3, y 3) は×印を付して表している。DVD-ROM72を初めて製造したとき、全ての公開鍵及び暗号化鍵Qは有効とされている。しかしながら、例えば、公開鍵及び暗号化鍵Qの中の所定のもの (図12の第2の実施の形態の場合、key 3及び (x 3, y 3) に対応する暗号化鍵Q) が第3者に破られしまったような場合、その公開鍵及び暗号化鍵Qに対応するフラグは無効として記録される。

【0069】なお、各公開鍵key 1, key 2, ke

y 3, ……………は、それぞれ公開鍵 ($\alpha 1, \beta 1, p 1$), ($\alpha 2, \beta 2, p 2$), ($\alpha 3, \beta 3, p 3$), ……………で構成されている。

【0070】このような公開鍵、暗号化された暗号化鍵Q及び有効フラグを表すキーテーブルが、DVD-ROM72のROM領域に記録されている場合には、このデータを書き換えることができないため、新しいバージョンのディスクとして、実質的に同一のコンテンツデータが記録されているディスクを新たに製造するときに、キーテーブルの有効フラグだけが書き換えられる。

【0071】制御部90は、駆動部91を制御し、駆動部91は、DVD-ROM72の所定のトラックに記録されているキーテーブルを読み出す。そして、この読み出したキーテーブルは制御部90に供給され、制御部90は、この読み出されたキーテーブルから、ステップS31で受け取ったIDに対応する公開鍵、暗号化された暗号化鍵及びそれらに対応するフラグを検出する。換言すれば、MPEGデコーダボード82の正規の製造者

(ボードメーカー) に対してはIDが予め与えられており、DVD-ROM72の製造者は、各IDに対応する公開鍵及び暗号化鍵Qを選定して、その公開鍵と公開鍵によって暗号化された暗号化鍵x、yをテーブルに記憶しておく。そこで、このステップS32で、各IDに対応する公開鍵及び暗号化された暗号化鍵x、yが検出される。

【0072】さらに、ステップS33において、この公開鍵及び暗号化された暗号化鍵に対応するフラグが有効とされているか否かを判定する。上述したように、例えば、不正コピーを行っているMPEGデコーダボード82の製造者 (ボードメーカー) に割り当てられているIDが発見された場合においては、そのIDに対応する公開鍵は無効とされる。そして、その発見後に製造されるDVD-ROM72に対応する公開鍵及び暗号化鍵Qは無効とするフラグが記録される。ステップS31で受け取ったIDに対応する公開鍵が無効と判定された場合、処理が終了される。すなわち、この場合においては、MPEGデコーダボード82は、DVD-ROM72の再生データを受け取ることができないことになる。なお、ここまでのデータの授受の流れが、図12に示されるKey exchangeに対応している。

【0073】一方、ステップ33において、ステップ31で受け取ったIDに対応する公開鍵が有効であると判定された場合、ステップS34に進み、制御部90は、第1に実施の形態と同様に、上述した式(1)からChallenge (C) を計算し、MPEGデコーダボード82の制御部100に供給する。

【0074】図12に示すように、このようにして計算されたChallenge (C) は、MPEGデコーダボード82の制御部100に供給される。制御部100は、図10のステップS52において、このChallenge (C) を

受け取る。そして、制御部100は、ステップS53に進み、第1の実施の形態と同様に、所定のランダムな番号k2を選択し、上述した式(2)、(3)からデジタルシグニチャr、dを演算し、その結果をResponse

(r、d)として、ディスクドライブ81に供給する。

【0075】図11に示すように、上述した式(2)及び(3)から求められたデジタルシグニチャr、dは、Response(r、d)として、ディスクドライブ81の制御回路90に供給される。制御部90は、図9のステップS35において、このResponse(r、d)を受け取り、ステップS36に進み、ステップ36において、このResponse(r、d)内のデジタルシグニチャr、dをチェックする。

【0076】すなわち、制御部90は、図12に示すように、 $\beta r \cdot rd$ を演算するとともに、 $\alpha C \bmod(p)$ を演算し、両者の値が等しいか否かを判定する。MPEGデコーダボード82が、正規のデコーダである場合、第1の実施の形態と同様に、デジタルシグニチャr、dと公開鍵 β とを用いて演算される値 $\beta r \cdot rd$ の値は、Challenge(C)、公開鍵 α 、pを用いて求められる値 $\alpha C \bmod(p)$ の値と等しくなる。逆に、MPEGデコーダボード12が正規のデコーダではない場合、両者の値は異なるものとなる。この場合、制御部90の処理は終了される。従って、この場合、DVD-ROM72のビデオデータはMPEGデコーダボード82に出力されないことになる。

【0077】ステップS36において、演算された2つの値が等しいと判定された場合、ステップS37に進み、制御部90は、第1の実施の形態と同様に、Session Key Sを上述した式(4)より演算する(図12のSession Key S)。

【0078】一方、MPEGデコーダボード82の制御部90は、図10のステップS53において、Response(r、d)を計算して、ディスクドライブ81に供給した後、ステップS54に進み、第1の実施の形態と同様に、ステップS52で受け取ったChallenge(C)を用いて上述した式(5)に従って、Session Key S'を演算する(図12のSession Key S*)。

【0079】よって、ステップS37においてディスクドライブ81の制御部90によって計算されたSession Key Sと、ステップS54においてMPEGデコーダボード82の制御部100によって演算されたSession Key S'は、第1の実施の形態で説明したように、それぞれ上述した式(6)及び(7)で表され、両者は等しい値となる。すなわち、ディスクドライブ81とMPEGデコーダボード82において、それぞれ同一の暗号化鍵が得られたことになる。

【0080】さらに、ディスクドライブ11において、Session Key Sを演算すると、ステップS38に進み、駆動部91は、DVD-ROM72より再生された暗号

化された暗号化鍵x、yを、そのままMPEGデコーダボード82に供給する(図12のx、y(as is))。

【0081】MPEGデコーダボード82の制御部100は、Session Key S'が得られたら、次にステップS55に進み、ステップ38において、暗号化鍵復号部105がディスクドライブ81から供給された暗号化された暗号化鍵x、yを受け取るように制御し、また、メモリ103から秘密鍵nを読み出して、暗号化鍵復号部105に供給し、次に、ステップS56に進む。ステップ56において、暗号化鍵復号部105は、暗号化された暗号化鍵x、yを次式(10)に従って復号(解読)し、この復号された暗号化鍵Q(復号鍵)が復号部104に供給される(図12のKey Decryption)。

$$Q = (y / x^n) \bmod(p) \quad \dots (10)$$

【0082】すなわち、暗号化鍵復号部105は、秘密鍵nと公開鍵pを用いて、暗号化されたx、yから暗号化鍵Qを復号(解読)する。

【0083】一方、ディスクドライブ81は、ステップS38で暗号化された暗号化鍵x、yをMPEGデコーダボード82に供給した後、さらに、ステップS39に進み、制御部90は、駆動部91を制御して、駆動部91は、DVD-ROM72から暗号化コンテンツデータを再生し、その再生された暗号化コンテンツデータ(暗号化鍵Qで暗号化されているコンテンツ)を暗号部92に供給するとともに、制御部90は、ステップS37で求めたSession Key Sを暗号化部92に供給する。暗号化部92は、再生された暗号化コンテンツデータをSession Key Sで暗号化して、暗号化データをMPEGデコーダボード82に供給する(図12のEncryption)。

【0084】MPEGデコーダボード82の復号部101は、図10のステップS55において、暗号化部92から供給された暗号化データを受け取り、ステップS56において、その暗号化データを、ステップS54で求めたSession Key S'を用いて復号(解読)する(図12のDecryption)。上述したように、Session Key S'は、Session Key Sと同一の値であるので、正しい復号(暗号の解読)を行うことができる。これにより、Session Key Sによる暗号化が解除され、暗号化鍵Qで暗号化されている暗号化コンテンツデータが得られることになる。そして、この暗号化コンテンツデータが復号部104に供給される。

【0085】次にステップS59に進み、復号部104は、復号部101からの暗号化コンテンツデータを復号部104からの復号(解読)された暗号化鍵Q(復号鍵)を用いて復号(解読)する。すなわち、第2の実施の形態の場合、DESの復号処理が実行される(図12のDecryption)。そして、この復号(解読)された符号化されているコンテンツデータ(符号化コンテンツデータ)がMPEGデコード部102に供給される。

【0086】MPEGデコード部102は、復号部10

4によって復号(解読)された符号化コンテンツデータを受け取り、この符号化コンテンツデータをMPEG方式で復号し、この復号されたコンテンツデータをモニタ3に供給する(図12のDecode)。そして、モニタ73は、このコンテンツデータを再生画像として図示しない表示画面に表示する。

【0087】以上、上述したように、第2の実施の形態においては、ディスクに記録されているコンテンツデータが暗号化されており、さらに、ディスクドライブ81において、このコンテンツデータが暗号化される(つまり、コンテンツデータが2重に暗号化されている)ため、ディスクドライブ81とMPEGデコーダボード82間のデータを傍受したとしても、第1の実施の形態の効果に比べて、不正コピーはより困難になる。

【0088】また、このように、この第2の実施の形態においては、セッションキーSを求めるとき用いられる公開鍵 α 、 p と、認証処理(識別処理)を行うとき用いられる公開鍵 β とを用いて、コンテンツを暗号化する暗号化鍵Qを暗号化するようにしたので、暗号化のために必要となる鍵の数を減らすことができる。すなわち、暗号化鍵Qを、公開鍵 α 、 β 、 p 以外の鍵を用いて暗号化することも可能であるが、そのようにすると鍵の数が増加し、鍵が破られた場合において、鍵を変更する(無効とする)処理が困難になる。そこで、この第2の実施の形態のように、セッションキーSと認証に用いられる公開鍵 α 、 β 、 p を、コンテンツを暗号化する暗号化鍵Qの暗号化にも共通に用いるようにすることにより、鍵の数を減らすことができる。

【0089】また、第2に実施の形態において、ディスクドライブ内の制御部90は、暗号化部92と一体化して構成してもよい。また、MPEGデコーダボード内の制御部100は、復号部101、104及び105と一体化して構成してもよい。

【0090】さらに、第2の実施の形態においては、MPEGデコーダボード82からIDをディスクドライブ81に供給し、ディスクドライブ81において認証を行うようにしたが、ディスクドライブ81からIDを供給し、MPEGデコーダボード82において認証を行うようにしてもよい。また、ディスクとして、DVD-ROMを用いる場合を例としたが、本発明は、その他の記録媒体に記録されているデータを再生する場合にも適用することができる。なお、ディスクがRAMタイプのディスクである場合、制御部90は、所定の指令が入力されたとき、そのフラグを無効なフラグに書き換えることも可能である。

【0091】なお、上記第1及び第2の実施の形態においては、図6、図7、図12に示すように、暗号化された公開鍵 x 、 y を、公開鍵 α 、 β 、 p とともにまとめて1つのキーテーブルに登録するようにしたが、例えば図13に示すように、暗号化された暗号化鍵 x 、 y を、フ

ラグとともにIDに対応して、公開鍵 α 、 β 、 p のキーテーブルとは別のキーテーブルにまとめるようにすることも可能である。

【0092】さらに、上記第1及び第2の実施の形態においては、上記した鍵の生成に1方向性関数を用いるようにすることが可能である。この1方向性関数を用いて鍵の生成方法は、本出願人によって、例えば、特願平8-269502号として先に提案されているものを用いることができる。

【0093】以上、上記第1及び第2の実施の形態においては、本発明をディスクドライブとデコーダとの間における暗号化鍵の交換と認証を例として説明したが、本発明はこれに限らず、その他の装置に適用することも可能である。例えば、ディスクドライブを、ネットワークを介してデコーダにデータを伝送するセンタに置き換え、センタとデコーダの間において、本発明を適用することもできる。

【0094】また、上記第1及び第2の実施の形態においては、記録されるコンテンツデータの一例として、ビデオデータを用いて説明しているが、本発明はこれに限らず、オーディオデータ、プログラムデータもしくはその他のデータに適用することが可能である。

【0095】さらに、上記第1及び第2の実施の形態においては、MPEG方式のエンコード及びデコードを例として説明したが、本発明はこれに限らず、他の符号化方式によるエンコード及びデコードを適用することも可能である。

【0096】また、本発明の第1及び第2の実施の形態は、ブロック図を用いてハードウェアとして表現しているが、本発明はこれに限らず、CPUやメモリなどを用いてソフトウェアで実現することも可能である。

【0097】なお、本発明の主旨を逸脱しない範囲において、さまざまな変形や応用例が考えうる。従って、本発明の要旨は、実施の形態に限定されるものではない。

【0098】

【発明の効果】以上、上述したように、本発明におけるデータ復号方法およびデータ復号装置によれば、一方は、他方から供給されるデジタルシグニチャ r とランダムな値 k_1 を用いて暗号化鍵を演算し、他方は、チャレンジ C とランダムな値 k_2 を用いて暗号化鍵を演算するようにし、このデジタルシグニチャ r を公開鍵 α 、 p とランダムな値 k_2 を用いて演算するようにしたので、暗号化鍵が破られ難くなり、データの不正なコピーを確実に防止することが可能となる。

【0099】また、本発明における認証方法によれば、デジタルシグニチャ r 、 d と、所定の公開鍵 β とを用いて演算される値と、公開鍵 α 、 p とチャレンジ C を用いて演算される値とを比較して、その比較結果に対応して認証を行うようにしたので、より安全な認証システムを構築することが可能となる。

【0100】さらに、本発明における記録媒体、ディスク製造方法、記録方法及び記録装置によれば、暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p を、第1の装置または第2の装置を識別する識別データに対応して記録媒体に記録するようにしたので、データの不正なコピーを確実に防止することが可能な記録媒体を実現することができる。

【0101】また、本発明における記録媒体、ディスクの製造方法、記録方法及び記録装置によれば、第1の装置または第2の装置を識別するとき用いられる公開鍵 β を、識別データに対応して記録媒体に記録するようにしたので、より安全な認証システムを構築することが可能な記録媒体を実現することができる。

【0102】さらに、本発明における記録媒体、ディスク製造方法、記録方法及び請求項18に記載の記録装置によれば、データを暗号化する暗号化鍵Qを、暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p と、第1の装置または第2の装置を識別するとき用いられる公開鍵 β とを用いて暗号化した暗号化鍵 x 、 y を、第1の装置または第2の装置を識別する識別データに対応して記録する

【図面の簡単な説明】

【図1】本発明を適用した第1の実施の形態のパーソナルコンピュータの構成例を示すブロック図である。

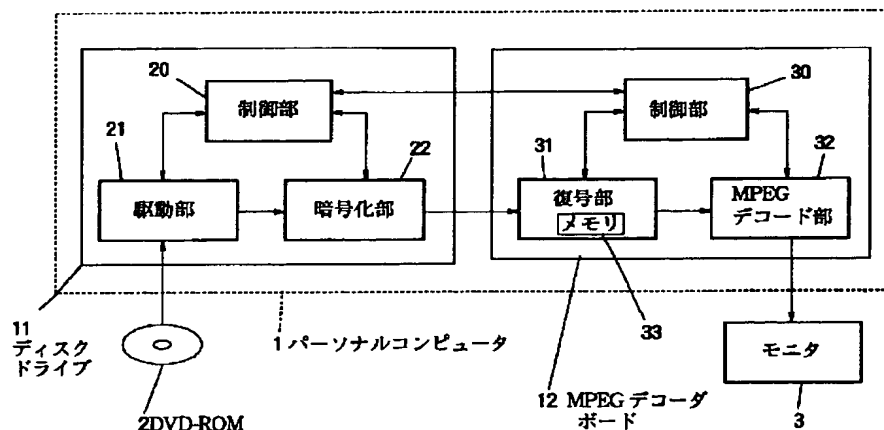
【図2】図1のディスクドライブの動作を説明するフローチャートである。

【図3】図1のMPEGデコーダボードの動作を説明するフローチャートである。

*

30

【図1】



*【図4】図1の第1の実施の形態の動作を説明するタイミングチャートである。

【図5】図1の第1の実施の形態におけるデータの流れを説明する模式図である。

【図6】本発明を適用した第1の実施の形態におけるDVD-ROMを製造する装置の構成例を示すブロック図である。

【図7】本発明を適用した第2の実施の形態におけるDVD-ROMを製造する装置の構成例を示すブロック図である。

【図8】本発明を適用した第2の実施の形態のパーソナルコンピュータの構成例を示すブロック図である。

【図9】図8のディスクドライブの動作を説明するフローチャートである。

【図10】図8のMPEGデコーダボードの動作を説明するフローチャートである。

【図11】図8の第2の実施の形態の動作を説明するタイミングチャートである。

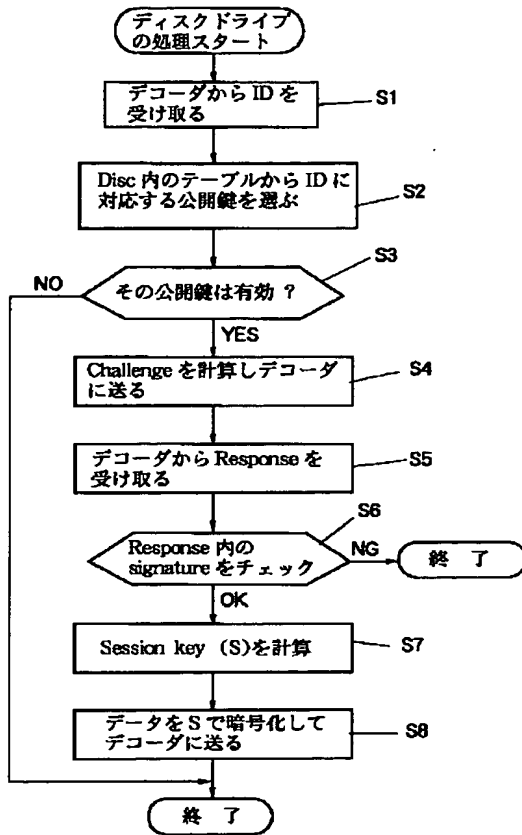
【図12】図8の第2の実施の形態におけるデータの流れを説明する模式図である。

【図13】コンテンツデータを暗号化した場合のキーテーブルの他の例を示す図である。

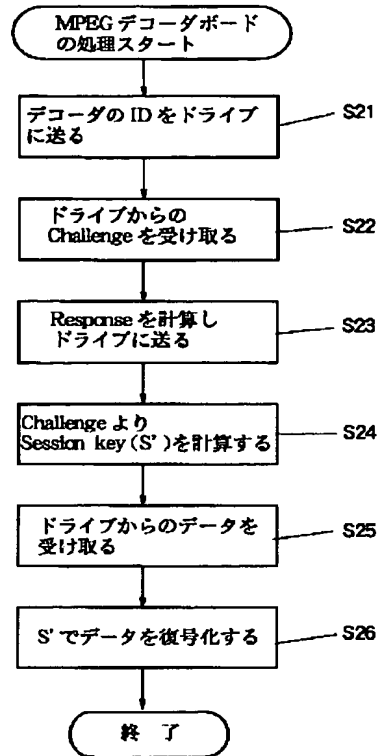
【符号の説明】

1 パーソナルコンピュータ、 2 DVD-ROM、
3 モニタ、 11 ディスクドライブ、 12 MP
EGデコーダボード、 20 制御部、 21 駆動
部、 22 暗号化部、 30 制御部、 31 復号
部、 32 MPEGデコード部、 33 メモリ

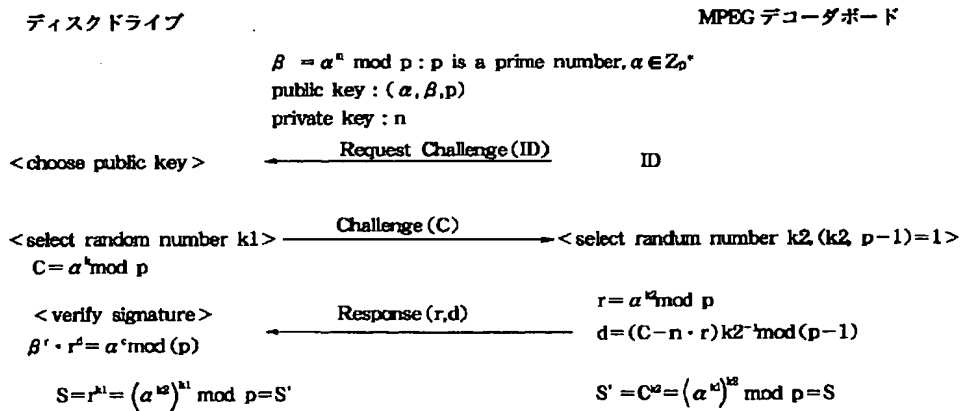
【図 2】



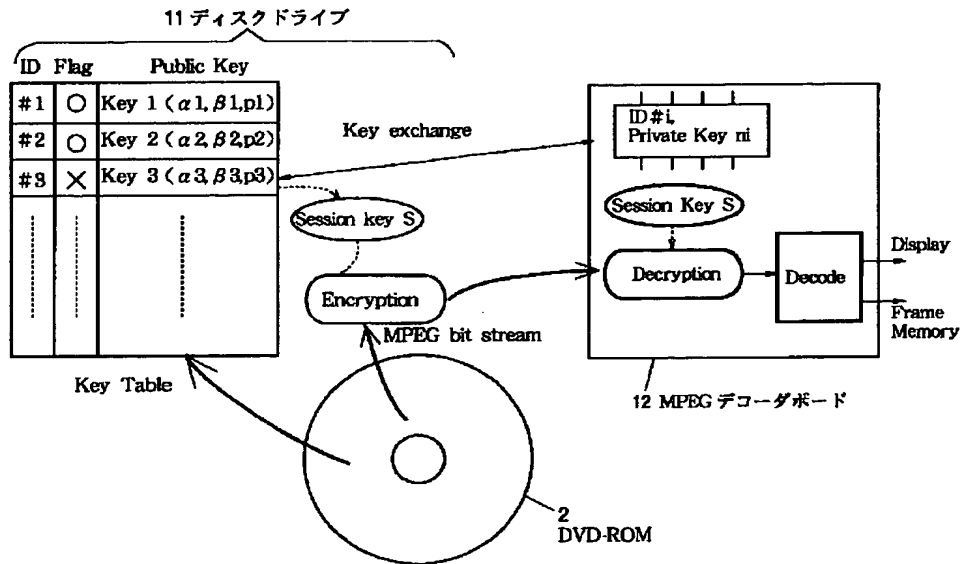
【図 3】



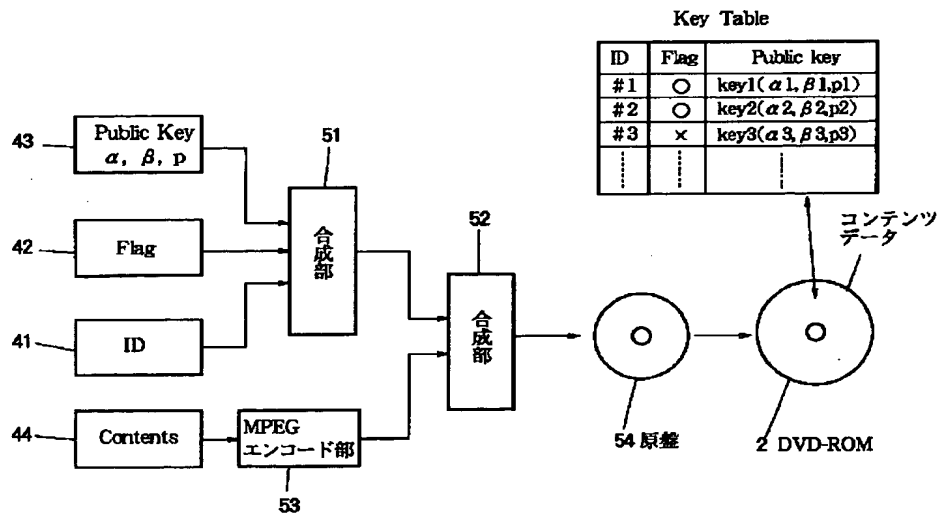
【図 4】



【図 5】



【図 6】

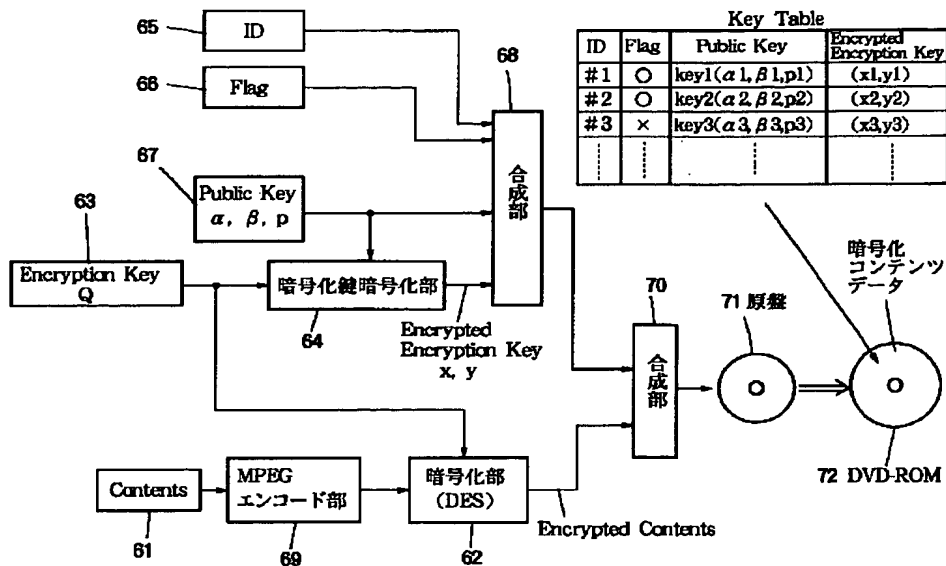


【図 13】

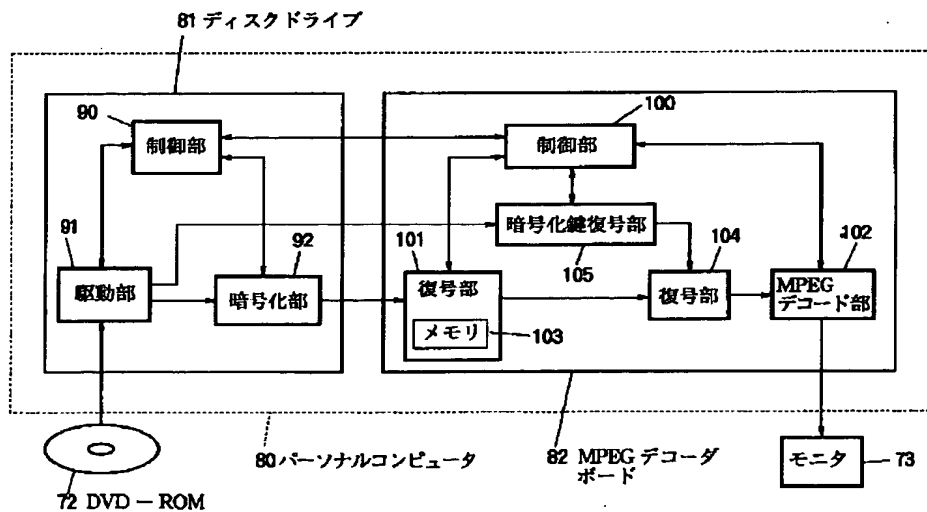
Key Table

ID	Flag	Encrypted Encryption key
#1	○	(x1, y1)
#2	○	(x2, y2)
#3	×	(x3, y3)
⋮	⋮	⋮

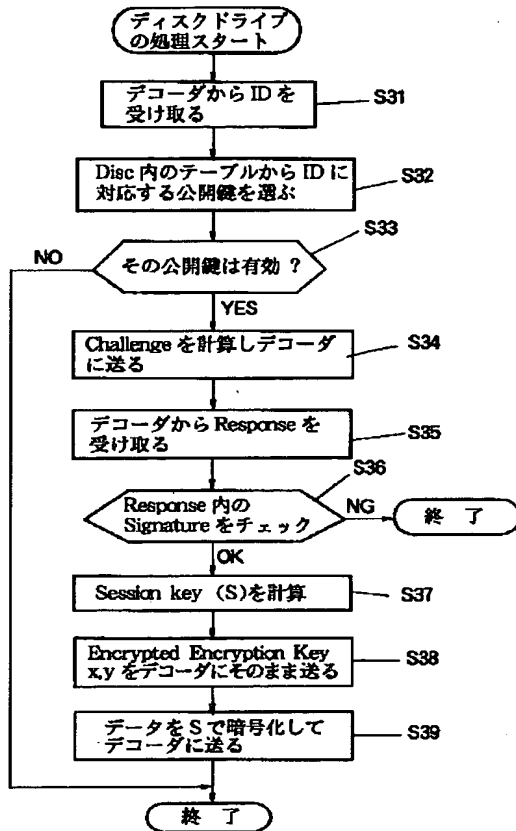
【図 7】



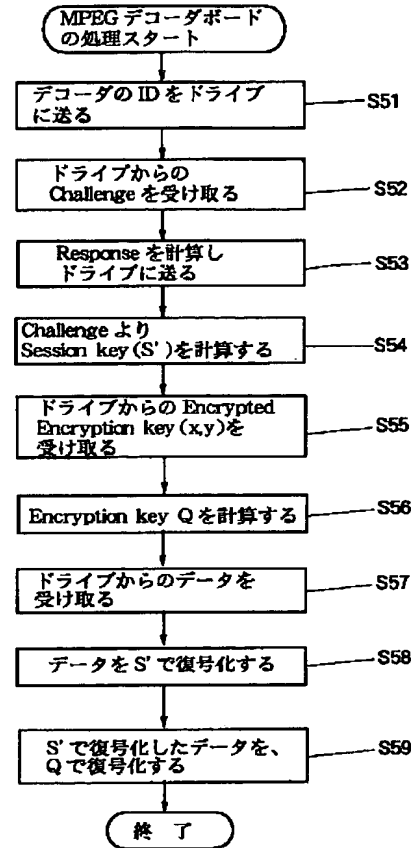
【図 8】



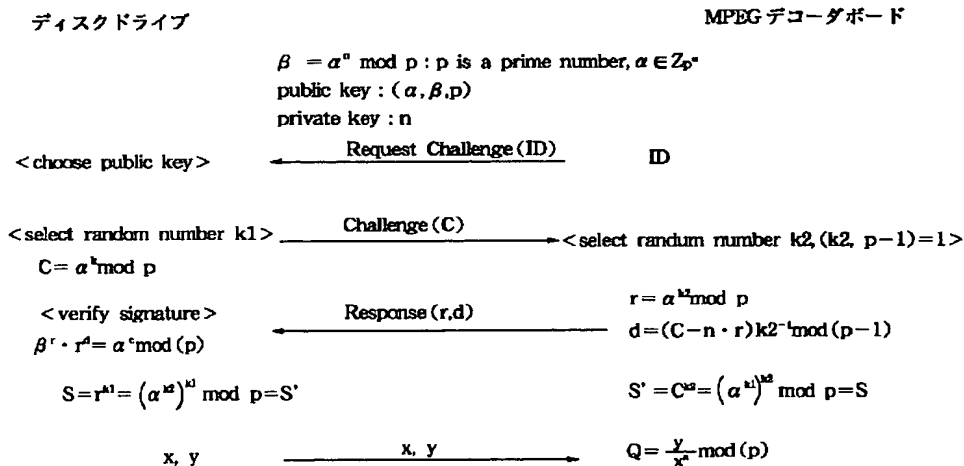
【図9】



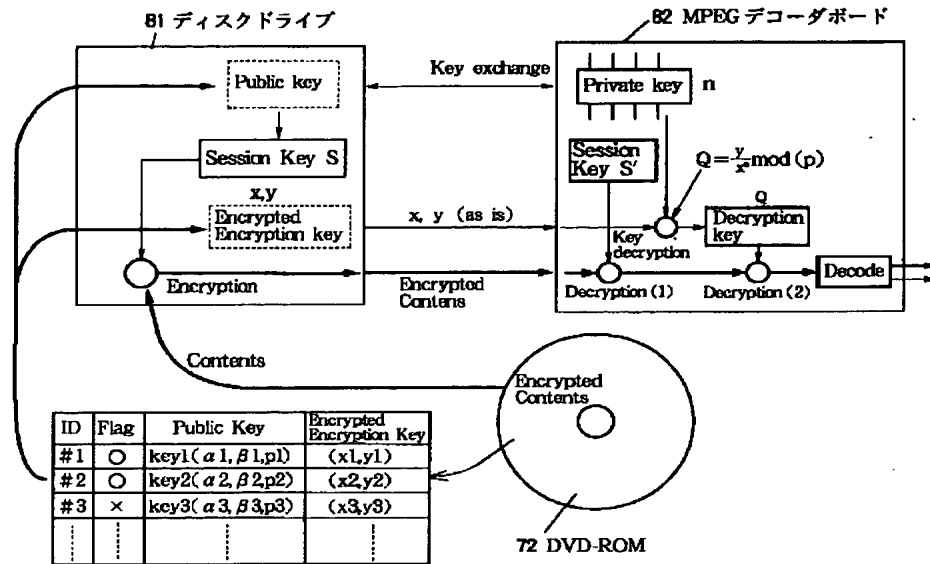
【図10】



【図11】



【図 1 2】



フロントページの続き

(51) Int. Cl. °

識別記号 庁内整理番号

F I

H 0 4 N 7/13

技術表示箇所

Z